ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow: Maria Naya Plasencia
Visited Location : FHNW, Windisch, Switzerland
Duration of Visit: 9 months

I - Scientific activity
(1 page at maximum)

During my 9 months stay at the FHNW with Professor Willi Meier, I have worked, as planned, on symmetric cryptography. In particular, I have followed two main research threads.

- Analysis and follow-up of the SHA-3 competition candidates:

Hash functions are one of the three branches in symmetric cryptography. They take a message of arbitrary length and return a fixed size digest. They have many applications, like authentication, digital signatures and fingerprinting. Due to recent attacks, the confidence in the actual standard has been undermined, and that is why the American Institute of Standards and Technology has launched in 2008 a public competition for finding a new standard, SHA-3. Nowadays this competition is at the end of the second round with 14 candidates standing out of the 64 submitted ones. It's then of main importance that the cryptographic community analyze and study these algorithms. I am coauthor of one of the 14 remaining algorithms: Shabal. Jointly with part of the Shabal team I have studied some properties of the internal permutation of Shabal and have been able to include them in the security proof. This result will be presented at the Second SHA-3 conference organized by the NIST. Also, I have participated on the analysis of two other second round candidates: Shavite-256, Shavite-512 and Luffa, obtaining results that have been published in several conferences.

- NLFSR based algorithms:

The non-linear feedback shift registers are widely used in symmetric cryptography algorithms due to several advantages like their compactness and speed. Because of this, their study is of main importance. During my stay I worked with these registers in two ways:
-We have designed a NLFSR-based lightweight hash function: Quark. The hash functions participating at the SHA-3 competition are not designs to be used in applications where really small hash functions are needed, like RFID tags or sensor networks. There is a need of this type of hash functions that had not yet been covered. Quark, that has been accepted at the top conference on the field, CHES, proposes a good solution for these cases.
-We have proposed a new framework for analyzing NLFSR based algorithms: the conditional differential cryptanalysis. With this, we have been allowed to give the best known results on the stream cipher Grain-80, a finalist of the ECRYPT NoE eSTREAM project which is actually implemented, recovering several keybits for the biggest number of rounds so far (104 out of 160). It is possible to combine our method with higher order differentials, allowing us then to obtain also the best known results on Grain-128, recovering also some bits of the key. This work has been submitted to Asiacrypt 2010.

More detailed information about each paper is given in the abstracts of the next section.

II- Publication(s) during your fellowship

Please insert the title(s), author(s) and abstract(s) of the published paper(s). You may also mention the paper(s) which were prepared during your fellowship period and are under reviewing.

[1] P. Gauravaram, G. Leurent, F. Mendel, M. Naya-Plasencia, T. Peyrin, C. Rechberger, and M. Schläffer. Cryptanalysis of the 10-round hash and full compression function of SHAvite-3-512. In Africacrypt 2010, LNCS. Springer, 2010. 18 pages, to appear.

Abstract:

In this paper, we analyze the SHAvite-3-512 hash function, as proposed and tweaked for round 2 of the SHA-3 competition. We present cryptanalytic results on 10 out of 14 rounds of the hash function SHAvite-3-512, and on the full 14 round compression function of SHAvite-3-512. We show a second preimage attack on the hash function reduced to 10 rounds with a complexity of 2497 compression function evaluations and 216 memory. For the full 14-round compression function, we give a chosen counter, chosen salt preimage attack with 2384 compression function evaluations and 2128 memory (or complexity 2448 without memory), and a collision attack with 2192 compression function evaluations and 2128 memory.

[2] J-Ph. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia. QUARK : a lightweight hash. In CHES 2010, LNCS. Springer, 2010. 13 pages, to appear.

Abstract:

The need for lightweight cryptographic hash functions has been repeatedly expressed by application designers, notably for implementing RFID protocols. However not many designs are available, and the ongoing SHA-3 Competition probably won't help, as it concerns general-purpose designs and focuses on software performance. In this paper, we thus propose a novel design philosophy for lightweight hash functions, based on a single security level and on the sponge construction, to minimize memory requirements. Inspired by the lightweight ciphers Grain and KATAN, we present the hash function family Quark, composed of the three instances u-Quark, d-Quark, and t-Quark. Hardware benchmarks show that Quark compares well to previous lightweight hashes. For example, our lightest instance u-Quark conjecturally provides at least 64-bit security against all attacks (preimages, multicollisions, distinguishers, etc.), fits in 1379 gate-equivalents, and consumes in average 2.44 μW at 100 kHz in 0.18 μm ASIC. For 112-bit security, we propose t-Quark, which we implemented with 2296 gate-equivalents.

[3] D. Khovratovich, M. Naya-Plasencia, A. Röck, and M. Schläffer. Cryptanalysis of luffa v2 components. In SAC 2010, LNCS. Springer, 2010. 22 pages, to appear.

Abstract:

We develop a number of techniques for the cryptanalysis of the SHA-3 candidate Luffa, and apply them to various Luffa components. These techniques include a new variant of the rebound approach taking into account the specifics of Luffa. The main improvements include the construction of good truncated differential paths, the search for differences using multiple inbound phases and a fast final solution search via linear systems. Using these techniques, we are able to construct non- trivial semi-free-start collisions for 7 (out of 8 rounds) of Luffa-256 with a complexity of 2104 in time and memory. This is the first analysis of a Luffa component other that the permutation of Luffa v1. Additionally, we provide new and more efficient

distinguishers also for the full permutation of Luffa v2. For this permutation distinguisher, we use a new model which applies first a short test on all samples and then a longer test on a smaller subset of the inputs. We demonstrate that a set of right pairs for the given differential path can be found significantly faster than for a random permutation.

[4] E. Bresson, A. Canteaut, T. Fuhr, T. Icart, M. Naya-Plasencia, P. Paillier, J. Reinhard, and M. Videau. Internal distinguishers in indifferentiable hashing : The Shabal case. In The second SHA-3 candidate conference, Santa Barbara, USA, 2010.
Abstract:

We show the first indifferentiability proof of a hash construction C F which does not make the assumption that the inner primitive F is ideal, but allows the existence (up to certain bounds that we explicit) of statistical distinguishers on F. Our hash construction is a general domain extender that generalizes both Chop-MD and Shabal and we prove that this general mode of operation is indifferentiable from a random oracle by providing tight security bounds when the inner primitive F is either an ideal compression function or a keyed permutation. Our proof provides the tightest possible security bounds on Chop-MD and even improves the original indifferentiability proof of Shabal. We then extend our results to the case where F is not assumed ideal anymore, but presents some (possibly strong) form of statistical bias in its input-output behavior. Our results allow us to derive new indifferentiability bounds for Shabal and show that the series of recently found (order-1, differential or rotational) distinguishers on its internal keyed permutation leave fully intact its indifferentiability properties.

[5] S. Knellwolf, W. Meier and M. Naya-Plasencia. Conditional Differential Cryptanalysis of NLFSR-based Cryptosystems . Submitted to Asiacrypt 2010.
Abstract:

Non-linear feedback shift registers are widely used in lightweight cryptographic primitives. For such constructions we propose a general analysis framework based on differential cryptanalysis. The essential idea is to identify conditions on the internal state to obtain a deterministic differential characteristic for a large number of rounds. Depending on whether these conditions involve public variables only, or also key variables, we derive distinguishing and partial key recovery attacks. We apply these methods to analyse the security of the eSTREAM finalist Grain v1 as well as the block cipher family KATAN/KTANTAN. This allows us to distinguish Grain v1 reduced to 104 of its 160 rounds and to recover some information on the key. The framework naturally extends to higher order differentials and enables us to distinguish Grain-128 up to 215 of its 256 rounds and to recover parts of the key up to 213 rounds. All results are the best known thus far and are achieved by experiments in practical time.

[6] M. Minier, M. Naya-Plasencia and T. Peyrin. Distinguishers on the Reduced-round SHAvite-3-256 Compression Function . Submitted to CT-RSA 2010.
Abstract:

In this article, we provide the first independent analysis of the tweaked 256-bit version of the SHA-3 candidate SHAvite-3. By leveraging recently introduced cryptanalysis tools such as rebound attack or Super-Sbox cryptanalysis, we are able to derive distinguishing attacks on the compression function on up to 8 rounds (12 rounds in total) and free-start collisions on up to 6 rounds. In particular, our best results are obtained by carefully controlling the differences in the key schedule of the internal cipher.

III -Attended Seminars, Workshops, and Conferences

Please identify the name(s), date(s) and place(s) of the events in which you participated during your fellowship period.

- Lightweight working group organized by ECRYPT. Leuven, Belgium. (January 2010)
- SHA-3 cryptanalysis working group organized by ECRYPT. Paris, France. (April 2010)
- NCCR MICS Workshop. EPFL, Lausanne, Switzerland. (Juin 2010)
- Conference: SAC 2010, Waterloo. (August 2010)
- Conference: Crypto 2010, Santa Barbara. (August 2010)
- Conference: CHES 2010, Santa Barbara. (August 2010)
- Second SHA-3 conference, Santa Barbara. (August 2010)

IV – Research Exchange Programme (12 month scheme)

Please identify the name(s), date(s) and place(s) of your Research Exchanges during your fellowship period and detail them .

Not applicable